LibreOffice? Aber sicher!

Praktische Betrachtung der IT-Sicherheit von LibreOffice

OPENSOURCE SECURITY

Penetrationstests

Beratung

Schulung

https://os-s.net

OPENSOURCE SECURITY

Sicherheitsstudie mit dem BSI

Empfehlung zur sicheren Konfiguration von LibreOffice

Online abrufbar[1]

Ergebnisse in diesem Vortrag :)

1) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/_/infos/20220819_BSI-CS_146_147.html

AGENDA

Angriff

Verteidigung

Optimierungspotenzial

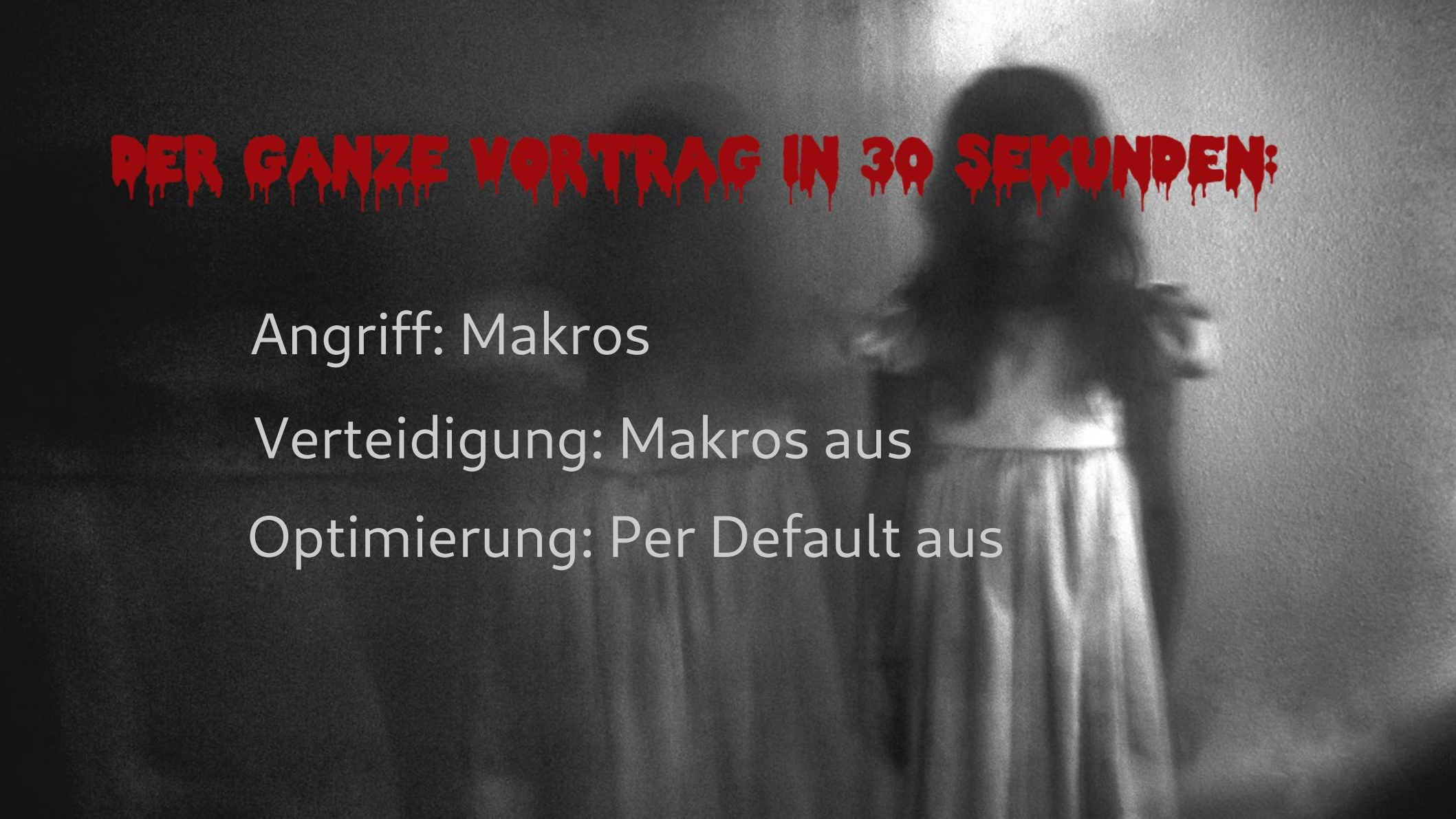
ANGRIFF

Wie gehen Angreiferinnen und Angreifer vor?

Welche Ziele wollen sie erreichen?

MITRE ATT&CK studieren


MAKROS



Der ganze Vortrag in 30 Sekunden:

Angriff: Makros

Verteidigung: Makros aus

Optimierung: Per Default aus

ANGRIFF

Wir haben mehr als 30 Sekunden!

Also etwas detaillierter...

ANGRIFF

Schadsoftware ausführen

Aktive Inhalte einbetten

Schwachstellen ausnutzen

Erweiterung installieren/ausführen

ANGRIFF

Sammeln von Informationen

Benutzerverhalten auswerten

Dokumenteninhalt einsehen

Systeminformationen sammeln

Zugangsdaten sammeln

ANGRIFF

Umgehen von Schutzmaßnahmen

Social Engineering

Identifizierung des Schadcodes erschweren

ANGRIFF

Persistenz

Dauerhafter Zugang zu dem System

ANGRIFF

Demo

VERTEIDIGUNG

VERTEIDIGUNG

Sichere Konfiguration erstellen

36 sicherheitsrelevante Konfigurationswerte

17 Abweichungen zur Standardkonfiguration

Geringe Komplexität im Vergleich mit MS-Office

VERTEIDIGUNG

Makros deaktivieren

vollständig

VERTEIDIGUNG

Angriffsoberfläche reduzieren

Ungenutzte Dateiformate deaktivieren

Erweiterung abschalten

Update-Check-Intervall herabsetzen

VERTEIDIGUNG

Nachladen von Inhalten verhindern

Nicht für alle Inhalte möglich

VERTEIDIGUNG

Nutzung des Passwortspeichers verhindern

VERTEIDIGUNG

Privacy

Senden von Nutzungsberichten deaktivieren

Crash-Reporter abschalten

VERTEIDIGUNG

Konfigurationsformate

dconf (nur Linux)

Gruppenrichtlinien (nur Windows)

XML-Files (Linux, Windows, MacOS)

VERTEIDIGUNG

Beispiel XML-Files

Datei erstellen

Im gewünschten Pfad ablegen

OPTIMIERUNGSPOTENZIAL

OPTIMIERUNGSPOTENZIAL

Macro Sicherheit

Deaktivieren per Default oder

SecurityLevel erhöhen

Ausführungsumgebung vergleichbar mit dem Webbrowser

OPTIMIERUNGSPOTENZIAL

Kommunikation

Blockieren von externen Verknüpfungen
Deaktivieren unsicherer Netzwerkprotokolle

OPTIMIERUNGSPOTENZIAL

Updates

Automatische Installation von Updates

Updates für Extensions

OPTIMIERUNGSPOTENZIAL

Deaktivierung wenig genutzter Features

LibreLogo

DDE-Befehle/OLE-Objekte

Dateiformate

Kontakt

info@os-s.de

www.os-s.de

Ressourcen

Download XML-Referenzkonfiguration

https://os-s.net/research/libreoffice

Sichere Konfiguration für LibreOffice beim BSI

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/_/infos/20220819_BSI-CS_146_147.html

Sichere Konfiguration für Microsoft Office beim BSI

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2019/Empfehlungen_Microsoft_190619.html

ATTACK

https://attack.mitre.org

LibreOffce Konfigurationsformate

https://wiki.documentfoundation.org/Deployment_and_Migration